AMENDMENT TO THE CLAIMS

Sub B2

A3

1. (Currently amended) A method for sharing a secure communication session with a client between a plurality of servers, comprising:

receiving a message from the client at a first server in the plurality of servers, the message including a session identifier that identifies a secure communication session with the client; and

if the session identifier does not correspond to an active secure communication session on the first server, establishing an active secure communication session with the client on the first server by,

attempting to retrieve state information associated with the session identifier for an active secure communication session between the client and a second server from the plurality of servers,

if the state information for the active secure communication session is retrieved, using the state information to establish the active secure communication session with the client without having to communicate with the client, whereby the secure communication session is transferred from the client and the second server to the client and the first server without incurring the overhead of establishing a new secure connection, and

if the state information for the active secure communication session is not retrieved, communicating with the client to establish the active secure communication session with the client.

2. (Original) The method of claim 1, wherein attempting to retrieve the state information includes:

Sub B2

attempting to use the session identifier to identify the second server in the plurality of servers that has an active secure communication session with the client that corresponds to the session identifier; and

attempting to retrieve the state information from the second server.

3. (Original) The method of claim 1, wherein attempting to retrieve the state information involves attempting to retrieve the state information from a centralized repository that is in communication with the plurality of servers.

4. (Original) The method of claim 3, wherein the centralized repository includes a database for storing the state information.

A3

5. (Original) The method of claim 1, wherein establishing the active secure communication session involves establishing a secure sockets layer (SSL) connection with the client.

6. (Original) The method of claim 1, wherein the state information includes:

a session encryption key for the secure communication session;

the session identifier for the secure communication session; and

a running message digest for the secure communication session.

7. (Original) The method of claim 6, further comprising:

using the message to update the running message digest; and

checkpointing the updated running message digest to a location outside of the first server.

Sub B2

8. (Original) The method of claim 1, further comprising, if the state information for the active secure communication session is retrieved, purging the state information from a location from which the state information was retrieved, so that the state information cannot be subsequently retrieved by another server in the plurality of servers.

9. (Original) The method of claim 1, further comprising initially establishing an active secure communication session between the client and the second server, the active secure communication session being identified by the session identifier.

A3

10. (Original) The method of claim 1, wherein attempting to retrieve the state information includes authenticating and authorizing the first server.

11. (Cancelled)

12. (Cancelled)

13. (Currently amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for sharing a secure communication session with a client between a plurality of servers, the method comprising:

receiving a message from the client at a first server in the plurality of servers, the message including a session identifier that identifies a secure communication session with the client; and

if the session identifier does not correspond to an active secure communication session on the first server, establishing an active secure communication session with the client on the first server by,

Sub B^2

attempting to retrieve state information associated with the session identifier for an active secure communication session between the client and a second server from the plurality of servers,

if the state information for the active secure communication session is retrieved, using the state information to establish the active secure communication session with the client without having to communicate with the client, whereby the secure communication session is transferred from the client and the second server to the client and the first server without incurring the overhead of establishing a new secure connection, and

A3

if the state information for the active secure communication session is not retrieved, communicating with the client to establish the active secure communication session with the client.

14. (Original) The computer-readable storage medium of claim 13, wherein attempting to retrieve the state information includes:

attempting to use the session identifier to identify the second server in the plurality of servers that has an active secure communication session with the client that corresponds to the session identifier; and

attempting to retrieve the state information from the second server.

15. (Original) The computer-readable storage medium of claim 13, wherein attempting to retrieve the state information involves attempting to retrieve the state information from a centralized repository that is in communication with the plurality of servers.

Sub B^2

16. (Original) The computer-readable storage medium of claim 15, wherein the centralized repository includes a database for storing the state information.

17. (Original) The computer-readable storage medium of claim 13, wherein establishing the active secure communication session involves establishing a secure sockets layer (SSL) connection with the client.

18. (Original) The computer-readable storage medium of claim 13, wherein the state information includes:

a session encryption key for the secure communication session;

the session identifier for the secure communication session; and

a running message digest for the secure communication session.

A^3

19. (Original) The computer-readable storage medium of claim 18, wherein the method further comprises:

using the message to update the running message digest; and

checkpointing the updated running message digest to a location outside of the first server.

20. (Original) The computer-readable storage medium of claim 13, wherein the method further comprises, if the state information for the active secure communication session is retrieved, purging the state information from a location from which the state information was retrieved, so that the state information cannot be subsequently retrieved by another server in the plurality of servers.

Sub B2

21. (Original) The computer-readable storage medium of claim 13, wherein the method further comprises initially establishing an active secure communication session between the client and the second server, the active secure communication session being identified by the session identifier.

22. (Original) The computer-readable storage medium of claim 13, wherein attempting to retrieve the state information includes authenticating and authorizing the first server.

23. (Cancelled)

A3

24. (Cancelled)

25. (Currently amended) An apparatus that shares a secure communication session with a client between a plurality of servers, comprising:

a receiving mechanism, at a first server in the plurality of servers, that receives a message from the client, the message including a session identifier that identifies a secure communication session with the client;

an examination mechanism that examines the session identifier; and

a session initialization mechanism, on the first server, wherein if the session identifier does not correspond to an active secure communication session on the first server, the session initialization mechanism is configured to establish an active secure communication session with the client by,

attempting to retrieve state information associated with the session identifier for an active secure communication session between the client and a second server from the plurality of servers,

Sub B2

if the state information for the active secure communication session is retrieved, using the state information to establish the active secure communication session with the client without having to communicate with the client, whereby the secure communication session is transferred from the client and the second server to the client and the first server without incurring the overhead of establishing a new secure connection, and

if the state information for the active secure communication session is not retrieved, communicating with the client to establish the active secure communication session with the client.

A3

26. (Original) The apparatus of claim 25, wherein the session initialization mechanism is configured to attempt to retrieve the state information by:

attempting to use the session identifier to identify the second server in the plurality of servers that has an active secure communication session with the client that corresponds to the session identifier; and

attempting to retrieve the state information from the second server.

27. (Original) The apparatus of claim 25, wherein the session initialization mechanism is configured to attempt to retrieve the state information by attempting to retrieve the state information from a centralized repository that is in communication with the plurality of servers.

28. (Original) The apparatus of claim 27, wherein the centralized repository includes a database for storing the state information.

Sub B^2

29. (Original) The apparatus of claim 25, wherein the active secure communication session includes a secure sockets layer (SSL) connection with the client.

30. (Original) The apparatus of claim 25, wherein the state information includes:

a session encryption key for the secure communication session;

the session identifier for the secure communication session; and

a running message digest for the secure communication session.

A^5

31. (Original) The apparatus of claim 30, further comprising an updating mechanism that is configured to:

use the message to update the running message digest; and to

checkpoint the updated running message digest to a location outside of the first server.

32. (Original) The apparatus of claim 25, further comprising a purging mechanism that is configured to purge the state information from a location from which the state information was retrieved, so that the state information cannot be subsequently retrieved by another server in the plurality of servers.

33. (Original) The apparatus of claim 25, wherein the session initialization mechanism is configured to authenticate and authorize the first server prior to receiving the state information.

34. (Cancelled)

35. (Cancelled)